Pure Storage FlashBlade 4.4.8.post1

Security Target

Evaluation Assurance Level (EAL): EAL2

Doc No: 2272-002-D102
Version: 3.4
30 October 2025

Pure Storage, Inc.
2555 Augustine Dr.
Santa Clara, CA 95054

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview, and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Pure Storage FlashBlade 4.4.8.post1 Security Target
ST Version:	3.4
ST Date:	30 October 2025

1.3 TOE REFERENCE

TOE Identification:	Purity OS 4.4.8.post1 running on the FlashBlade //E, FlashBlade //S200, or FlashBlade //S500 Models
TOE Developer:	Pure Storage Inc.
TOE Type:	Storage Device, Other Devices and Systems

1.4 TOE OVERVIEW

The TOE is the Purity OS 4.4.8.post1 running on the FlashBlade //E, FlashBlade //S200, or FlashBlade //S500. Pure Storage FlashBlade (FB) provides managed all flash file and object storage. This allows for traditional hierarchical storage where information is accessed based on its path and object storage where data is accessed based on an identifier and associated metadata. FlashBlade provides both the performance advantage of file storage and the scalability advantage of object storage. File store access is supported via NFS/SMB clients and object store access is supported by S3 clients.

The evaluated FlashBlade//E system contains one control chassis and an expansion chassis. Each chassis may contain up to ten blades with each blade containing up to four DirectFlash Modules (DFMs). External Fabric Modules (XFMs) interconnect chassis and connect to clients via the data center network.

The evaluated FlashBlade//S200 and S500 systems contain one control chassis. The chassis may contain up to ten blades with each blade containing up to four DirectFlash Modules (DFMs). The two models are functionally equivalent. The S200 is optimized for efficiency and the S500 is optimized for performance.

The blades run the Purity//FB software which executes client and administrative commands to manage flash storage for the entire system. Management is performed via a CLI (over SSH) or GUI (over HTTPS). The user is responsible for ensuring that the data network suitably protects NFS/SMB traffic between the FlashBlade and the clients.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following software, hardware and networking components are required for operation of the TOE in the evaluated configuration.

Component	Software	Hardware
Administrator Workstation	Windows 10 with Chrome 118.0 or later, or Firefox 119.0 or later	General Purpose Computer Hardware
LDAP Server or AD Server	Microsoft Server 2016 and	General Purpose Computer

Component	Software	Hardware
supporting Kerberos authentication and TLS v1.2 or TLS v1.3.	later.	Hardware
NTP Server	Software supporting NTP version 4 or later (RFC5905)	General Purpose Computer Hardware
Syslog server	Software supporting RFC5424.	General Purpose Computer Hardware
Managed Switch (one per chassis)	Not applicable	Not applicable

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of two FlashBlade//E chassis connected by external fabric modules (xFMs) or a single FlashBlade//S200 or S500 chassis. Depending on the model, desired redundancy, and load one or two ethernet switches and xFMs provide connectivity to the LAN network. All three models use Purity OS 4.4.8.post1. The TOE and its components are shown in the following figures.

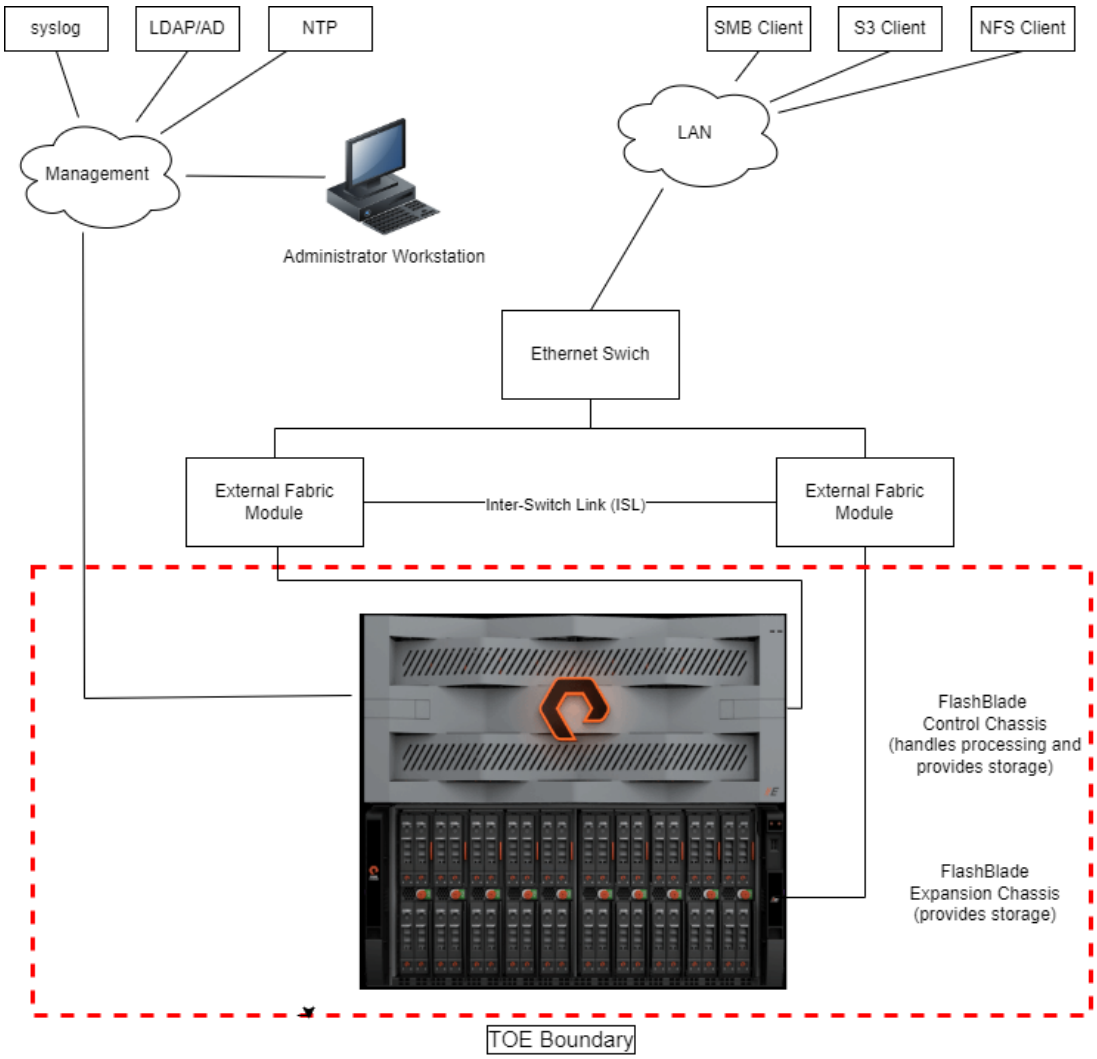

Figure 1 – FlashBlade //E

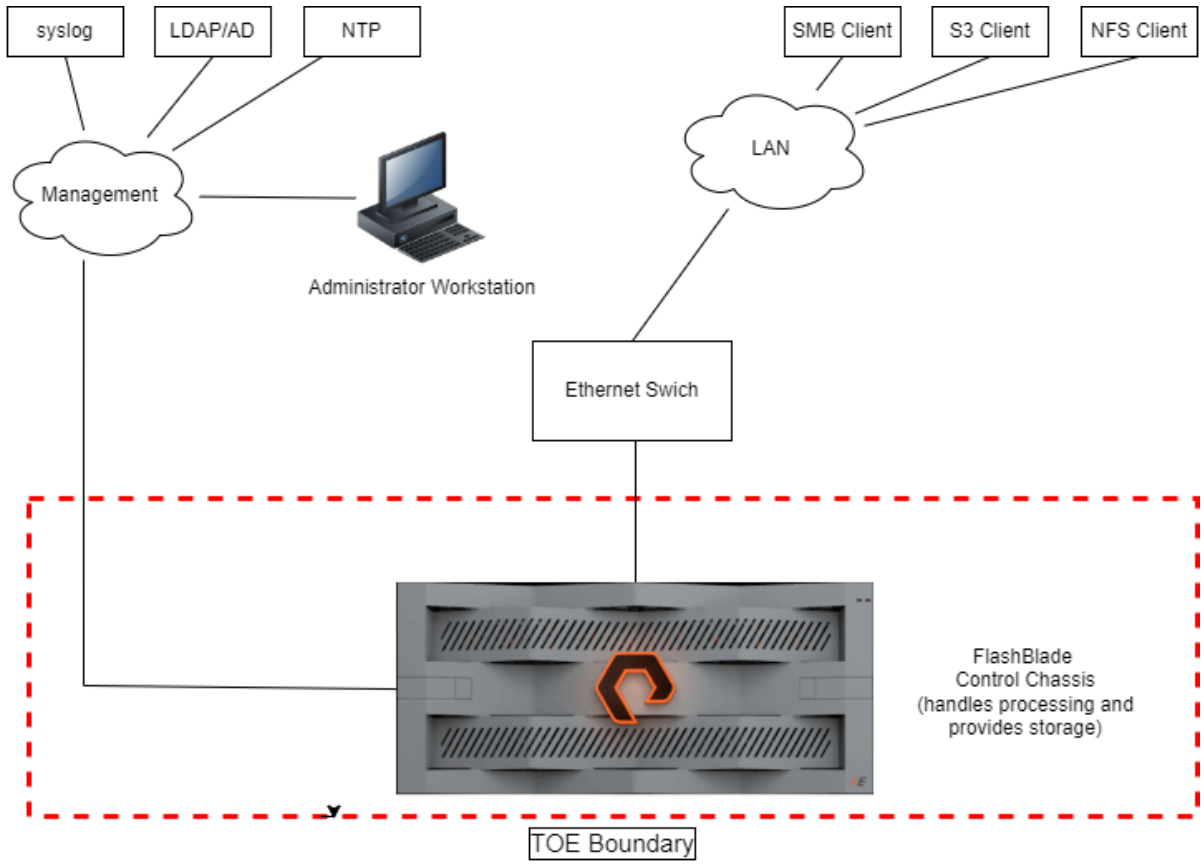

Figure 2 - FlashBlade //S

Each FlashBlade chassis consists of one to ten blades with each blade containing from one to four DFMs. The FlashBlade //E model contains two chassis. The FlashBlade//S models consist of a single chassis and do not use the external fabric modules. The component details are provided in the tables below.

TOE Component	Details
Control chassis	Model: CH-FB-II Blades: ○ Count 1-10 ○ Model: FB-EC ○ Processor: Intel Xeon Silver 4310 ○ DFMs (per blade): ■ Count: 1-4 Part Number: 83-0517-02
Expansion chassis	Model: CH-FB-II Blades: ○ Count 1-10 ○ Model: FB-EX ○ DFMs (per blade): ■ Count: 1-4 Part Number: 83-0517-02
eXternal Fabric Modules (xFM)	Count: 2 Model: EFM-3200e
Purity//FB software	Purity OS 4.4.8.post1

Table 2 - TOE Components for FlashBlade//E

TOE Component	Details
Control chassis	Model: CH-FB-II Blades: ○ Count 1-10 ○ Model: FB-S200 ○ Processor: Intel Xeon Silver 4310 ○ DFMs (per blade): ■ Count: 1-4 Part Number: 83-0443-02
Purity//FB software	Purity OS 4.4.8.post1

Table 3 - TOE Components for FlashBlade//S200

TOE Component	Details
Control chassis	Model: CH-FB-II Blades: ○ Count 1-10 ○ Model: FB-S500 ○ Processor: Intel Xeon Silver 4316 ○ DFMs (per blade): ■ Count: 1-4 Part Number: 83-0443-02
Purity//FB software	Purity OS 4.4.8.post1

Table 4 - TOE Components for FlashBlade//S500

1.5.1.1 TOE Delivery

The TOE hardware with a base version of the software is shipped via a commercial freight courier to the address provided by the customer. The customer receives the following:

- Two FlashBlade//E chassis with two external fabric (XFM) modules, FlashBlade//S200, or FlashBlade//S500.
- Documentation is available to registered customers on the Pure Storage support site (https://support.purestorage.com/FlashBlade).

The blades, DFMs, and software are preinstalled in the chassis. The external fabric modules must be installed and connected by the customer. The customer is responsible for obtaining and connecting the managed switches. Pure Storage provides a list of switches that they have tested. Configuration and integration of the TOE hardware is performed by the support engineers or an authorized partner.

Upgrading and configuration of the TOE software version is normally performed by developer support engineers. The Common Criteria Guidance Supplement is provided directly to the customer by Pure Storage support.

1.5.1.2 TOE Guidance

The TOE includes the following documentation:

- FlashBlade//E Quick Installation Guide, 40-0323-01
- FlashBlade//E Multi-Chassis Installation Guide, 50-0046-04
- FlashBlade//S Quick Installation Guide, 40-0284-02
- FlashBlade//S Single Chassis Installation Guide, 50-0030-01
- FlashBlade//S Multi-Chassis Quick Installation Guide, 50-0041-01
- FlashBlade//S Multi-Chassis Installation Guide. 50-0040-05
- FlashBlade User Guide Version, 4.4.2
- FlashBlade Command Line Interface Reference, Version 4.4.2

- FlashBlade Object Store S3 REST API 2.3
- FlashBlade 4.4.8.post1 Common Criteria Guidance Supplement

Registered customers can obtain the documentation on the Pure Storage support site.

1.5.2 Logical Scope

The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 5 – Logical Scope of the TOE below summarizes the logical scope of the TOE.

Functional Class	Description
Identification and Authentication (FIA)	Administrators must identify and authenticate prior to TOE access. The TSF enforces a failure limit and passwords are not revealed during authentication.
Protection of the TSF (FPT)	Reliable timestamps are provided in support of audit record creation.
Security Audit (FAU)	Audit entries are generated for security related events. The audit logs are protected from unauthorized modification, unauthorized deletion, and may be reviewed by authorized administrators. Viewed audit records can be sorted and filtered. Timestamp information is provided to support auditing. An audit log storage duration and record limit are also enforced.
Security Management (FMT)	The TOE provides management capabilities via a web based GUI (via HTTPS) and CLI (via SSH). Management functions allow the administrators to configure system and network settings, configure users and roles, and perform other TOE functions. The storage administrator (or array administrator) can also configure user access to the array's file and object storage. Access via SMB, S3, and NFS clients is supported.
TOE Access (FTA)	A banner is presented on user login. Administrator sessions can be locked or terminated by both the user and

Functional Class	Description
	TSF. Establishment of sessions can be restricted to specific IP addresses.
Trusted Path/Channel (FTP)	The communications links between the TOE and its remote administrators are protected using HTTPS (TLS v1.2 or TLS v1.3) for the Web GUI or SSH v2 for the CLI. TLS v1.2 is used to protect communication to the remote audit log server. The LDAP connection is protected by TLS v1.2 or TLS v1.3.
User Data Protection (FDP)	The TOE provides managed storage to NFS, SMB, and S3 clients.

Table 5 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- HTTP access to file systems
- Use of Pure1 Remote Assistance and logging
- Ops Admin role
- Use of the local console interface
- NFS ACLs and ACEs
- Pure file safemode
- Pure object safemode
- S3 object lock
- Bandwidth throttling for replication
- File system usage limits
- File system snapshots
- Fast remove
- Quotas
- Object replication
- File system replication
- Analysis
- Administration using the REST API
- Health monitoring
- Enterprise key management (EKM) servers
- Key management interoperability protocol (KMP)
- Alerts

The following are not supported:

- NFSv4.1 pNFS, Delegation, Referrals, and Share reservation
- SMBv1

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

The TOE is CC Part 2 conformant and CC Part 3 conformant. The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been considered.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE to any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 6 – Threats lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attackers is assumed to be unsophisticated.

TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters but are assumed not to be wilfully hostile.

Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.
T.COMPDATA	An unauthorized individual may attempt to access or alter TSF data or user data stored by the TOE by circumventing security.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

Table 6 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no security rules, procedures, or guidelines imposed on the operational environment.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 7 – Assumptions

Assumption	Description
A.LOCATE	The TOE and LDAP/AD server will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile.

Table 7 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.
O.TIME	The TOE must provide reliable timestamps.

Table 8 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.PERSON	Personnel working as authorized administrators shall be selected to be careful, attentive, non-hostile, and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from any physical attack.

Table 9 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

Objective	A.LOCATE	A.MANAGE	A.NOEVIL	T.ACCOUNT	T.COMPDATA	T.UNDETECT
O.ACCESS				X	X	
O.ADMIN				X	X	
O.AUDIT						X
O.TIME						X
OE.PERSON		X	X			
OE.PHYSICAL	X					

Table 10 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat	Objective	Rationale
T.ACCOUNT: An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.	O.ACCESS	O.ACCESS contributes to the mitigation of this threat by ensuring that only authorized administrator have access to TSF data and that users of the TOE's services do not have access to TSF data.
T.ACCOUNT: An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.	O.ADMIN	O.ADMIN ensures the management of the TOE configuration is restricted to authorized personnel.
T.COMPDATA: An unauthorized individual may attempt to access or alter TSF data or user data stored by the TOE by circumventing security.	O.ACCESS	O.ACCESS contributes to the mitigation of this threat by ensuring that access to user and TSF data is controlled.
T.COMPDATA: An unauthorized individual may attempt to access or alter TSF data or user data stored by the TOE by circumventing security.	O.ADMIN	O.ADMIN contributes to the mitigarion of this threat by restricting access to TOE functions and data.
T.UNDETECT: Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	O.AUDIT	O.AUDIT contributes to the mitigation of this threat by ensuring that audit records are available.
T.UNDETECT: Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	O.TIME	The TOE provides reliable timestamps for use in the audit records.

Table 11 - Rational for Objectives Related to Threats

4.3.2 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption	Objective	Rationale
A.LOCATE: The TOE and LDAP/AD server will be located within controlled access facilities, which will prevent unauthorized physical access.	OE.PHYSICAL	OE.PHYSICAL supports this assumption by ensuring that authorized administrators provide for physical protection of the TOE and the LDAP/AD server.
A.MANAGE: There are one or more competent individuals assigned to manage the TOE.	OE.PERSON	OE.PERSON supports this assumption by ensuring that TOE administrators are knowledgeable in managing the TOE, are careful, attentive, and non-hostile.
A.NOEVIL: The authorized administrators are not careless, willfully negligent, or hostile.	OE.PERSON	OE.PERSON supports this assumption by ensuring that the TOE administrators are careful, attentive, and non-hostile.

Table 12 - Rational for Objectives Related to Assumptions

4.3.3 Security Objectives Rationale Related to OSPs

There are no security rules, procedures, or guidelines imposed on the operational environment.

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control' and 'FDP_ACC.1(2) Subset access control'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 13.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control
	FDP_ACC.1(2)	Subset access control
	FDP_ACC.1(3)	Subset access control

Class	Identifier	Name
	FDP_ACC.1(4)	Subset access control
	FDP_ACF.1(1)	Security attribute based access control
	FDP_ACF.1(2)	Security attribute based access control
	FDP_ACF.1(3)	Security attribute based access control
	FDP_ACF.1(4)	Security attribute based access control
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes
	FMT_MSA.1(2)	Management of security attributes
	FMT_MSA.1(3)	Management of security attributes
	FMT_MSA.1(4)	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialisation
	FMT_MSA.3(2)	Static attribute initialisation
	FMT_MSA.3(3)	Static attribute initialisation
	FMT_MSA.3(4)	Static attribute initialisation
	FMT_MTD.1	Management of TSF data

Class	Identifier	Name
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
Trusted Path/Channel (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 13 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*the events listed in Table 14 - Auditable Events*].

Note: The TOE does not allow its administrator to reboot the OS or start/shut down the audit functions.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*user interface, and command details*].

SFR	Auditable Event
FIA_UAU.2	Logins and unsuccessful authentication attempts are audited for the GUI and CLI.
FIA_UID.2	Logins and unsuccessful authentication attempts are audited for the GUI and CLI.
FMT_MSA.1(1)	Changes made to NFS export rules are audited.
FMT_MSA.1(2)	Changes to SMB client rules are audited.
FMT_MSA.1(3)	Changes to SMB share rules are audited.
FMT_MSA.1(4)	Changes to object store access rules are audited.
FMT_SMR.1	An audit record is created when a user's role assignment is changed.
FPT_STM.1	Changes to the NTP server settings.
FTA_TSE.1	Changes to the IP address restrictions.

Table 14 - Auditable Events

Note: Invalid commands are rejected but are not logged. For a Web GUI login failure the TOE records the interface rather than the username.

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*FlashBlade administrators*] with the capability to read [*all*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*sorting and filtering*] of audit data based on [*sorting of a single audit record field and filtering of a*

logical AND combination of audit record fields consisting of ID, time, user, command, subcommand, arguments, location, and user interface].

6.2.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

6.2.1.6 FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [*delete the oldest audit trail entries*] if the audit trail exceeds [*1,000 records for the session log and 10,000 records for the audit log*].

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1(1) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*file system SFP*] on [

- *Subjects: file system clients,*
- *Objects: NFS mounts*
- *Operations: read, write*]

6.2.2.2 FDP_ACC.1(2) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*SMB Client SFP*] on [

- *Subjects: SMB clients,*
- *Objects: SMB file share*
- *Operations: read-only, read-write*]

6.2.2.3 FDP_ACC.1(3) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(3) The TSF shall enforce the [*SMB Share SFP*] on [

- *Subjects: SMB users,*
- *Objects: SMB file system*
- *Operations: read, write, delete, full control*]

6.2.2.4 FDP_ACC.1(4) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(4) The TSF shall enforce the [*object store SFP*] on [

- *Subjects: storage users,*
- *Objects: storage buckets and objects,*
- *Operations: get, list, create, put, delete*]

6.2.2.5 FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [*file system SFP*] to objects based on the following: [

- *Subjects: file system clients,*
- *Subject attributes: network identifier,*
- *Objects: NFS mounts*
- *Object attributes: protocol, NFS export rules and their index*].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *NFS export rules attached to each NFS mount determine if a file system client shall be granted read or write access to the NFS mount based on the file system client's network identifier,*
- *NFS export rules* are specified and ordered inside policies which are attached to mounts].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*by default NFS clients have read-write access to the NFS mount*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*a file system client will not have access if there is no NFS protocol enabled*].

6.2.2.6 FDP_ACF.1(2) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(2) The TSF shall enforce the [*SMB Client SFP*] to objects based on the following: [

- *Subjects: SMB clients,*
- *Subject attributes: SMB host name, FQDN, or IP address/subnet,*
- *Objects: SMB file shares,*
- *Object attributes: protocol, SMB client policies*].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *SMB client polices attached to each SMB file share determine if a SMB client shall be granted read-only or read-write access to the file system based on the SMB host name, FQDN, or IP address/subnet,*
- *client policies will be applied as they are ordered by their index*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*by default SMB clients have read-write access to the file system*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*a SMB client will not have access if there is no SMB protocol enabled*].

6.2.2.7 FDP_ACF.1(3) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(3) The TSF shall enforce the [*SMB Share SFP*] to objects based on the following: [

- *Subjects: SMB users,*
- *Subject attributes: username and group,*
- *Objects: SMB file systems,*
- *Object attributes:SMB share rules*].

FDP_ACF.1.2(3) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *SMB share rules attached to each SMB share determine if a SMB user shall be granted read-only, read-write, or full control access to the SMB share based on the SMB user's username and group,*
- *SMB share rules for a client will be applied as they are ordered by their index*].

FDP_ACF.1.3(3) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*default SMB share rules assigned allows SMB users full access to the file system*].

FDP_ACF.1.4(3) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

6.2.2.8 FDP_ACF.1(4) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(4) The TSF shall enforce the [*object store SFP*] to objects based on the following: [

- *Subjects: storage users,*
- *Subject attributes: storage account identifier and access key*
- *Objects: storage buckets and objects,*
- *Object attributes: object store access rules consisting of S3 get, list, create, put, and delete actions*].

FDP_ACF.1.2(4) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *Object store access rules attached to each storage bucket and object determine if a storage user shall be granted access to the bucket and object based on the storage account name identifier, access key, and the assigned S3 action(s)*].

FDP_ACF.1.3(4) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(4) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*if a request does not match any rules then the request is implicitly denied, in the case of multiple rules a deny rule will take precedence over an allow rule*]].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*1 to 100*]] unsuccessful authentication attempts occur related to [*Web GUI and CLI authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block password based logins for the user for a configurable time*].

6.2.3.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password, role*].

Note: For Web GUI and CLI administrators the TOE has a single default pureuser. For additional administrator accounts the username and password are maintained by the LDAP server.

6.2.3.3 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note: This applies to Web GUI and CLI users. Storage user actions are controlled by the file system SFP, SMB Client SFP, SMB Share SFP, and object store SFP.

6.2.3.4 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*dots or no feedback*] to the user while the authentication is in progress.

Note: This applies to Web GUI and CLI users and is not applicable for TOE storage users.

6.2.3.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [*defined in FMT_SMF.1 (Table 16 - Management Activities)*] to [*the authorised identified roles defined in the same table*]

6.2.4.2 FMT_MSA.1(1) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(1) The TSF shall enforce the [*file system SFP*] to restrict the ability to [query, modify, delete*,* [*create*]] the security attributes [

- *NFS export rules and their index*]

to [array_admin and *storage_admin role users*].

6.2.4.3 FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the [SMB *Client SFP*] to restrict the ability to [query, modify, delete*,* [*create*]] the security attributes [

- SMB client rules]

to [array_admin and *storage_admin role users*].

6.2.4.4 FMT_MSA.1(3) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(3) The TSF shall enforce the [SMB Share *SFP*] to restrict the ability to [query, modify, delete*,* [*create*]] the security attributes [

- SMB share rules]

to [array_admin and *storage_admin role users*].

6.2.4.5 FMT_MSA.1(4) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(4) The TSF shall enforce the [*object store SFP*] to restrict the ability to [query, modify, delete*,* [*create*]] the security attributes [

- *Object store access rules*]

to [array_admin and *storage_admin role users*].

6.2.4.6 FMT_MSA.3(1) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*file system SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.7 FMT_MSA.3(2) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*SMB Client SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.8 FMT_MSA.3(3) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(3) The TSF shall enforce the [*SMB share SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(3) The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.9 FMT_MSA.3(4) Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(4) The TSF shall enforce the [*object store SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(4) The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.10 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the operations listed in the table below*] **on** the [*TSF data in the table below*] to [*roles listed in the table below*].

TSF Data Type	Operation	Role
Storage user policies and rules	Create, Query, Modify, Delete	array_admin, storage_admin
	Query	readonly
Administrative User Roles	Create, Query, Modify, Delete	array_admin
	Query	readonly, storage_admin
Audit data	Query	readonly, storage_admin, array_admin
System configuration	Create, Query, Modify, Delete	array_admin
	Query	readonly, storage_admin
File and object store configuration	Create, Query, Modify, Delete	array_admin, storage_admin

TSF Data Type	Operation	Role
	Query	readonly

Table 15 - Access to TSF Data by Role

6.2.4.11 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management functions identified* in Table 16 - Management Activities].

SFR	Management Activity
FDP_ACC.1(1)	Users assigned to the array_admin or storage_admin role can administer the file system SFP controlling which file system clients have access to the NFS mounts.
FDP_ACC.1(2)	Users assigned to the array_admin or storage_admin role can administer the SMB client SFP controlling which SMB clients have access to the SMB file shares.
FDP_ACC.1(3)	Users assigned to the array_admin or storage_admin role can administer the SMB share SFP controlling which SMB users have access to the SMB file systems.
FDP_ACC.1(4)	Users assigned to the array_admin or storage_admin role can administer the object store SFP controlling which storage users have access to the storage buckets and objects.
FDP_ACF.1(1)	Users assigned to the array_admin or storage_admin role can administer the file system SFP controlling which file system clients or users have access to the NFS mounts.
FDP_ACF.1(2)	Users assigned to the array_admin or storage_admin role can administer the SMB client SFP controlling which object protocol clients or users have access to the SMB shares.
FDP_ACF.1(3)	Users assigned to the array_admin or storage_admin role can administer the SMB share SFP controlling which object protocol clients or users have access to the SMB shares.
FDP_ACF.1(4)	Users assigned to the array_admin or storage_admin role can administer the object store SFP controlling which object protocol clients or users have access to the storage objects.
FIA_AFL.1	Users assigned to the array_admin role can configure the threshold.
FIA_UAU.2	Users assigned to the array_admin role are responsible for

SFR	Management Activity
	maintaining the administrative users.
FIA_UID.2	Users assigned to the array_admin role are responsible for maintaining the administrative users.
FMT_MTD.1	A user assigned to the array_admin role can configure users and control which administrators belong to the storage administrator, readonly, and array_admin roles.
FMT_SMR.1	A user assigned to the array_admin role can configure administrator users and assign them to a role.
FPT_STM.1	A user assigned to the array_admin role can configure the connection to a NTP server.
FTA_SSL.3	A user assigned to the array_admin role can configure the inactive session timeout that applies to Web GUI and CLI sessions.
FTA_TAB.1	A user assigned to the array_admin role can configure the access banner.
FTA_TSE.1	A user assigned to the array_admin role can restrict administrator sessions to specific IP addresses.
FTP_ITC.1	Users assigned to the array_admin role can configure the syslog connection.

Table 16 - Management Activities

6.2.4.12 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*readonly, storage_admin, and array_admin*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive **Web GUI or CLI** session after a [*time interval of user inactivity defined by an administrator*].

6.2.6.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.6.3 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a **Web GUI or CLI** user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.6.4 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*IP address*].

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*remote syslog and LDAP*].

6.2.7.2 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*remote administration*].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance as defined in the CC Part 3. The assurance requirements are summarized in Table 17.

Assurance Class	Component Identifier	Component Name
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition

Assurance Class	Component Identifier	Component Name
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 17 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following table provides the mapping between the SFRs and Security Objectives.

SFR	O.ACCESS	O.ADMIN	O.AUDIT	O.TIME
FAU_GEN.1			X	
FAU_GEN.2			X	
FAU_SAR.1			X	
FAU_SAR.3			X	
FAU_STG.1			X	
FAU_STG.3			X	
FDP_ACC.1(1)	X			
FDP_ACC.1(2)	X			
FDP_ACC.1(3)	X			
FDP_ACC.1(4)	X			
FDP_ACF.1(1)	X			
FDP_ACF.1(2)	X			
FDP_ACF.1(3)	X			
FDP_ACF.1(4)	X			

SFR	O.ACCESS	O.ADMIN	O.AUDIT	O.TIME
FIA_AFL.1	X			
FIA_ATD.1	X			
FIA_UAU.2	X			
FIA_UAU.7	X			
FIA_UID.2	X			
FMT_MOF.1		X		
FMT_MSA.1(1)	X			
FMT_MSA.1(2)	X			
FMT_MSA.1(3)	X			
FMT_MSA.1(4)	X			
FMT_MSA.3(1)	X			
FMT_MSA.3(2)	X			
FMT_MSA.3(3)	X			
FMT_MSA.3(4)	X			
FMT_MTD.1	X			
FMT_SMF.1	X	X		
FMT_SMR.1	X	X		
FPT_STM.1			X	X
FTA_SSL.3		X		
FTA_SSL.4		X		
FTA_TAB.1	X	X		
FTA_TSE.1		X		
FTP_ITC.1	X			
FTP_TRP.1		X		

Table 18 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following table provides the rationale that traces each SFR back to the Security Objectives for the TOE.

Objective	SFR	SFR Description	Rationale
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACC.1(1)	Subset access control	FDP_ACC.1(1) supports this objective by limiting access to authorized NFS clients.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACC.1(2)	Subset access control	FDP_ACC.1(2) supports this objective by limiting access to authorized SMB clients.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACC.1(3)	Subset access control	FDP_ACC.1(3) supports this objective by limiting access to authorized SMB clients according to their policies.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACC.1(4)	Subset access control	FDP_ACF.1(4) supports this objective by restricting access to storage users.
O.ACCESS: The TOE must allow authorized servers	FDP_ACF.1(1)	Security attribute based access control	FDP_ACF.1(1) supports this objective by

Objective	SFR	SFR Description	Rationale
and users to access only appropriate TOE functions, TOE data, and user data.			restricting access to NFS mounts.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACF.1(2)	Security attribute based access control	FDP_ACF.1(2) supports this objective by restricting SMB client access.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACF.1(3)	Security attribute based access control	FDP_ACF.1(3) supports this objective by restricting SMB share access.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FDP_ACF.1(4)	Security attribute based access control	FDP_ACF.1(4) supports this objective by restricting access to storage buckets and objects.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FIA_AFL.1	Authentication failure handling	The TOE enforces authentication failure limits which helps to prevent unauthorized access.

Objective	SFR	SFR Description	Rationale
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FIA_ATD.1	User attribute definition	Their role as well as username/password are required for users accessing the TOE.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FIA_UAU.2	User authentication before any action	Authentication is required for all administrative users.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FIA_UAU.7	Protected authentication feedback	The TOE protects password entry which helps to prevent unauthorized access.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FIA_UID.2	User identification before any action	Authentication is required before users can access the TOE.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE	FMT_MSA.1(1)	Management of security attributes	This SFR ensures that only array_admin and stoarge_admin role users control the security attirbutes for NFS export

Objective	SFR	SFR Description	Rationale
data, and user data.			rules.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MSA.1(2)	Management of security attributes	This SFR ensures that only array_admin and stoarge_admin role users control the security attirbutes for SMB client rules.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MSA.1(3)	Management of security attributes	This SFR ensures that only array_admin and stoarge_admin role users control the security attirbutes for SMB share rules.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MSA.1(4)	Management of security attributes	This SFR ensures that only array_admin and stoarge_admin role users control the security attirbutes for object store access rules.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MSA.3(1)	Static attribute initialisation	This SFR enforces restrictive default values for the file system SFP.
O.ACCESS: The TOE must allow authorized servers and users to access only	FMT_MSA.3(2)	Static attribute initialisation	This SFR enforces restrictive default values for the SMB client SFP.

Objective	SFR	SFR Description	Rationale
appropriate TOE functions, TOE data, and user data.			
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MSA.3(3)	Static attribute initialisation	This SFR enforces restrictive default values for the SMB share SFP.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MSA.3(4)	Static attribute initialisation	This SFR enforces restrictive default values for the object store SFP.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_MTD.1	Management of TSF data	The TOE limits access to TSF data according to an administrator's role.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FMT_SMF.1	Specification of Management Functions	The TOE provides management functions that help an administrator maintain TOE security.
O.ACCESS: The TOE must allow authorized servers	FMT_SMR.1	Security roles	The FlashBlade has several roles which allow an

Objective	SFR	SFR Description	Rationale
and users to access only appropriate TOE functions, TOE data, and user data.			administrator to limit the functions a user can perform.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FTA_TAB.1	Default TOE access banners	This SFR supports the objective by ensuring that those who try to access the TOE are aware that only authorized users are permitted.
O.ACCESS: The TOE must allow authorized servers and users to access only appropriate TOE functions, TOE data, and user data.	FTP_ITC.1	Inter-TSF trusted channel	FTP_ITC.1 helps meet this objective by providing a trusted communication channel for audit records that protects data in transit from disclosure. This helps ensure that unauthorized users can't see the audit records.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1	Management of security functions behaviour	FMT_MOF.1 supports this objective by identifying the management functions that specific administrator roles are able to perform.
O.ADMIN: The TOE	FMT_SMF.1	Specification of	FMT_SMF.1

Objective	SFR	SFR Description	Rationale
will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.		Management Functions	supports this objective by identifying the management functions authorized administrators are able to perform.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_SMR.1	Security roles	FMT_SMR.1 meets this objective by supporting a list of authorized roles for the TOE.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FTA_SSL.3	TSF-initiated termination	This SFR supports this objective by terminating inactive sessions which protects against idle Web GUI and CLI sessions being used by unauthorized users.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in	FTA_SSL.4	User-initiated termination	This SFR supports this objective by allowing a user to end their session which protects against idle

Objective	SFR	SFR Description	Rationale
their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.			sessions being used by unauthorized users.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FTA_TAB.1	Default TOE access banners	This SFR supports the objective by ensuring that those who try to access the TOE are aware that only authorized users are permitted.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FTA_TSE.1	TOE session establishment	The TOE is able to restrict administrative session establishment to specific IP addresses thereby helping to prevent unauthorized access.
O.ADMIN: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and	FTP_TRP.1	Trusted path	The TOE uses a trusted path for administrator sessions which helps to prevent unauthorized access. This includes all methods of access encompassing the Web GUI and SSH

Objective	SFR	SFR Description	Rationale
facilities from unauthorized use.			CLI.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.	FAU_GEN.1	Audit data generation	This SFR outlines what data must be included in audit records and what events must be audited.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.	FAU_GEN.2	User identity association	FAU_GEN.2 supports this objective by associating a user identity with each auditable event generated.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.	FAU_SAR.1	Audit review	FAU_SAR.1 provides the means to review audit records.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the	FAU_SAR.3	Selectable audit review	Audit records can be viewed on all interfaces and in addition can be sorted and filtered

Objective	SFR	SFR Description	Rationale
resources protected by the TOE. The audit records must be viewable by administrative users.			in the Web GUI.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.	FAU_STG.1	Protected audit trail storage	Audit records for management activities are generated and stored on the TOE.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.	FAU_STG.3	Action in case of possible audit data loss	The TOE deletes the oldest audit trail entries that exceed 1,000 records which ensures that storage space is available for recent events.
O.AUDIT: The TOE must generate and store audit records for use of the TOE functions and the resources protected by the TOE. The audit records must be viewable by administrative users.	FPT_STM.1	Reliable time stamps	The TSF provides time stamps for the audit records.

Objective	SFR	SFR Description	Rationale
O.TIME: The TOE must provide reliable timestamps.	FPT_STM.1	Reliable time stamps	This SFR meets the objective by providing reliable timestamps for use in audit records.

Table 19 - Security Objectives and SFRs

6.4.3 Dependency Rationale

Table 20 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.3	FAU_STG.1	✓	
FDP_ACC.1(1)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(1).
FDP_ACC.1(2)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(2).
FDP_ACC.1(3)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(3).
FDP_ACC.1(4)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(4).
FDP_ACF.1(1)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(1).

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1).
FDP_ACF.1(2)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(2).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2).
FDP_ACF.1(3)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(3).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(3).
FDP_ACF.1(4)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(4).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(4).
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(1).

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(2).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(3).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(4)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(4).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2).
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2).
	FMT_SMR.1	✓	
FMT_MSA.3(3)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(3).
	FMT_SMR.1	✓	
FMT_MSA.3(4)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(4).
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	None	N/A	

SFR	Dependency	Dependency Satisfied	Rationale
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL.4	None	N/A	
FTA_TAB.1	None	N/A	
FTA_TSE.1	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 20 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 3.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

The TOE audits the events listed in Table 14 - Auditable Events. Invalid commands are rejected but are not logged. The 'Start up and shutdown of the audit function' audit record is captured as start up and shutdown messages for the TOE itself, since logging may not be started or stopped independently of powering on and powering off the TOE.

Logs can be read by FlashBlade administrators. Users of the TOE storage cannot access the logs. The logs are in two parts, a management network session log and an audit log. The management network session log contains the history of each access and access attempts to the FlashBlade and duration of each FlashBlade session. The audit log contains a chronological history of modification operations (for example, commands that create, update, and delete) that were run on the array.

The audit records contain the following fields:

- ID: The chronological number of the record.
- Time: The date and time the command was run.
- User: The user who ran the command.
- Command: The name of the command.
- Subcommand: The subcommand used with the command.
- Arguments: Any arguments used with the command and their associated user-supplied input.
- Location: The IP address where the command was issued.
- User Interface: The interface from which the operation was run. For example, CLI or GUI.

To prevent passwords being revealed in the audit log in cases where a user inadvertently enters their password in the username field the username is not logged for Web GUI failure attempts. The interface is logged.

Only successfully identified and authenticated administrators can view/read audit logs on the TOE. The audit logs can be viewed from the Web GUI and CLI and both interfaces provide sorting and filtering of audit data.

There is no provision to delete the audit logs. The TOE retains the last 1,000 audit records for the management network session log and 10,000 records for the audit log.

All audit records generated on the TOE are sent to a remote audit server (syslog server) over the TLS protected trusted channel. The audit records that are stored locally and those sent to the remote audit server are identical in content

and format. Locally generated audit records are sent to the remote audit server as soon as they are generated. If the trusted channel is not operational, then audit records will not be sent to the remote audit server; however, they will still be locally stored. The TSF does not queue up audit records that were not sent to the remote audit server for transmitting upon re-establishment of the trusted channel.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.3

7.2 USER DATA PROTECTION

User access is described below for the three clients.

7.2.1 NFS Clients

The TOE enforces the file system SFP on NFS clients connecting to the storage on the TOE. Client access is controlled by the file system network identifier which may be an IP address, host name, or net group. The protocol (NFSv3 or NFSv4.1) and NFS export rules define the access rights and privileges a client has to the file system's directories and files. The rules define client access to the directories and files as well as identifying the actions allowed (read or write). A user's access to an existing file or directory placed under the mount is governed by NFS ACLs and ACEs and is not part of the evaluation. The rules are specified and ordered inside policies which are attached to mounts.

When a file system is created with default arguments (i.e. no protocol is enabled), no NFS clients will have access because there is no NFS protocol. If no NFS Export Policy is specified during file system creation, the "NFS export rule string" of *(rw,no_root_squash) will be applied to the filesystem and NFS clients will have read-write access once the NFS protocol is enabled. If an NFS Export Policy is ever attached to a file system, either during creation or afterward, the above NFS Export String is removed.

If there is no NFS Export Policy and no NFS Export Rule String associated with a file system, then no access will be granted to NFS clients, even if an NFS protocol is enabled on the filesystem.

Having no rule that grants access to the client (including the case where there are no rules in the attached policy) results in the NFS client being unable to mount.

7.2.2 SMB Clients

The TOE enforces the SMB Client SFP and SMB Share SFP on SMB clients connecting to the storage on the TOE. Client access is controlled by SMB host name, FQDN, or IP address/subnet. SMB users are identified by username and group. The ability for clients to connect to a SMB share is determined by storage administrators as defined by SMB client rules and SMB share rules. The SMB protocol and SMB client rules manage the read and write privileges that an SMB client has to the file system. SMB share rules control SMB user permissions to

read and change files in the share to which they are attached or to control a file's ACL.

The _smb_client_allow_everyone and "_smb_share_allow_everyone" policies are both assigned to SMB shares by default and these allow all users full access A user from a client is not allowed access to SMB mount if there is no SMB client rule granting the client with appropriate access or if there is no SMB share rule granting the access. If either the SMB client policy or SMB share policy are missing, the mount is not accessible from the network. A SMB client will not have access if there is no SMB protocol enabled. Rules are applied as ordered by their index.

7.2.3 S3 Clients

The object store SFP is enforced on S3 users connecting to the storage on the TOE via object store access rules. Client user access is controlled by the storage account identifier (or access key ID), access key (secret), and object store access rules which are assigned as S3 actions. These actions are a collection of rules that control access to the objects. If an access request matches a rule it is allowed, otherwise the request is denied. In the case of multiple rules, a deny rule will take precedence over an allow rule.

The type of access (i.e. actions) allowed, is determined by the access policy attached to individual ID's respectively. In the context of object storage, "accounts" refers to the top-level organizational units or entities that manage and access data stored in buckets or containers within a specific object storage system. All storage user (S3 users) are TOE local user id's, created and managed by the storage/array admin, attached to individual accounts. A storage user is authenticated by the TOE based on its knowledge of the access key ID and secret access key. A successfully authenticated storage user is only allowed to access to buckets/objects group under the same "account". The type of access (i.e. actions) allowed, is determined by "Access Policy" attached to individual ID's respectively. By default, no "Access Policy" is attached to a new storage user ID during its creation.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACC.1(3), FDP_ACC.1(4), FDP_ACF.1(1), FDP_ACF.1(2), FDP_ACF.1(3), FDP_ACF.1(4)

7.3 IDENTIFICATION AND AUTHENTICATION

The identification and authentication function ensures that a user requesting a TOE administrative function has provided credentials and is authorized to access that service, based on the user's role. This applies to FlashBlade administrator authentication and is not related to user data plane authentication for clients. For Web GUI and CLI users the credentials consist of username and password.

For Web GUI and CLI connections the FlashBlade supports a single local user, named pureuser, with array-wide (array_admin) permissions. Users can be added to the array through LDAP by integrating the array with a directory service and assigning roles for one or more groups. Users can sign into the array

only if they are in a group that has been assigned a role. Role based access control for LDAP users is performed by configuring directory groups that correspond to the FlashBlade roles identified in Table 16 - Access to TSF Data by Role.

A bind user and bind password of a single service account is used by FlashBlade to search the directory server. User group assignments are managed within the LDAP/AD server. The user's group assignments in the directory server are used by the FlashBlade to assign the administrator user role. When a user submits a username/password combination, the TSF attempts to authenticate the user locally for the pureuser or via LDAP for other users. If the username/password combination match an authorized administrator’s credentials, the user is granted access to the web-based graphical user interface or CLI.

For the CLI, the TOE does not echo back the characters typed in for the password credential. In the administrative web GUI, the characters are echoed back as dots, effectively obscuring the password from shoulder-surfing.

The TSF can be administered through two interfaces which are the Web GUI or CLI. The Web GUI interface is protected by TLS v1.3 and insecure connections are redirected to https. The CLI interface is protected by SSHv2. The TSF requires that each administrative user be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

When a user connects to the Web GUI or CLI interface, the user is initially presented with the configured warning and consent banner, which the user must accept prior to continuing to the username/password authentication form.

If a Web GUI or CLI user enters an incorrect password enough times to meet the configured threshold (1-100 attempts), the offending user account will be prevented from successfully authenticating until a FlashBlade administrator defined time has elapsed (a configurable range of between 1 second and 90 days). The offending account will be locked out of both of the management interfaces. Failed authentication attempts are tracked using a monotonically incrementing counter. This counter is reset upon successful authentication of the offending account or after the administrator-defined time for account lockout has elapsed. To unlock a locked account, any administrator with the array_admin role that is not locked can issue a command at the SSH CLI interface to unlock the account.

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2

7.4 SECURITY MANAGEMENT

The TSF restricts the ability to query, modify, delete, or add security attributes to FlashBlade administrators that belong to an administrative role that has the appropriate privileges. The administrator roles are readonly, storage_admin, and array_admin.

- A read-only user has read-only privileges to run commands that convey the state of the array but cannot alter the state of the array.
- Storage Admin users have all the privileges of read-only users, plus the ability to run commands related to storage operations, such as administering file systems and object stores. This includes managing SMB client rules, SMB share rules, NFS export policies, NFS export rules, and object store access policies. Storage Admin users cannot perform operations that deal with global and system configurations.
- Array Admin users can perform all FlashBlade operations.

An administrative user's access to TSF data and the user's role relationship is provided in Table 15 - Access to TSF Data by Role. More details on the management activities are also in Table 16 - Management Activities.

Storage user access to user data is controlled by a user with the storage_admin role. By default, a storage user will not have access to array data unless granted by a storage administrator.

The array management directory service configuration is used to allow users within an LDAP server to manage the FlashBlade via the CLI or WEB GUI.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.3(1), FMT_MSA.3(2), FMT_MSA.3(3), FMT_MSA.3(4), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

7.5 PROTECTION OF THE TSF

The TOE has a hardware clock which can not be set from the CLI or Web GUI and must be synchronized with an external time server via network time protocol (NTPv4 or later). The TOE supports one or more NTP servers. The system clock is set to UTC and this is used for the following:

- audit logs.
- Web GUI and CLI session timeouts.
- input for the ‘Random’ field in the TLS Client_Hello and Server_Hello Handshake messages.

TOE Security Functional Requirements addressed: FPT_STM.1.

7.6 TOE ACCESS

Interactive Web GUI or CLI sessions are automatically logged out after a period of inactivity. A FlashBlade administrator can configure the timeout value from 1 second to 90 days.

Web GUI and CLI users can log out of their sessions.

An administrator configurable access banner is presented to Web GUI and CLI users prior to login.

Access to the administrative interfaces can be restricted to specific IP addresses. By default, there is no restriction and once one is defined it applies to the Web GUI and CLI. Changes apply to subsequent login attempts.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TSE.1.

7.7 TRUSTED PATH / CHANNELS

Communication with a remote audit log server is protected via TLS v1.2. TLS v1.2 or TLS v1.3 is used to protect the LDAP server connection. In all cases the connection is initiated by the TOE.

TLS v1.2 or TLS v1.3 is used for the Web GUI communication between the administrator workstation and the TOE's management interface. SSH v2 is used to create a trusted path between the CLI client and the TOE's management interface. In all cases the communication path is initiated by the remote user.

TOE Security Functional Requirements addressed: FTP_ITC.1, FTP_TRP.1

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
FlashBlade administrator	FlashBlade administrators control the FlashBlade according to their assigned roles and include users assigned to the readonly, storage_admin, or array_admin roles (see Table 15 - Access to TSF Data by Role). These are users who can login to the GUI or CLI.
Security Policy	The term security policy' is used in this ST to describe the policies implemented within the TOE to enforce the claimed functionality. It does not refer to the specific policies enforced by the User Data Protection SFRs.
Syslog	Syslog is a standard for logging messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them.

Table 21 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ACE	Access Control Entry
ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
DFM	DirectFlash Module
EAL	Evaluation Assurance Level
EFM	External Fabric Module
EKM	Enterprise Key Management
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface

Acronym	Definition
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
KMP	Key Management Interoperability protocol
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
OSP	Organisational Security Policy
pNFS	Parallel NFS
PP	Protection Profile
REST	Representational State Transfer
SDK	Software Development Kit
SFP	Security Function Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSE	TOE Session Establishment
TSF	TOE Security Function
UTC	Coordinated Universal Time
XFM	eXternal Fabric Module

Table 22 – Acronyms